College of Aerospace Doctrine, Research, and Education

IW 160

Computer Network Attack (CNA)

Computer Network Defense (CND)

Overview

- CNA
  - Definition
  - The Threat
  - The Arsenal
- CND
  - Definition
  - Structure
- Organizations

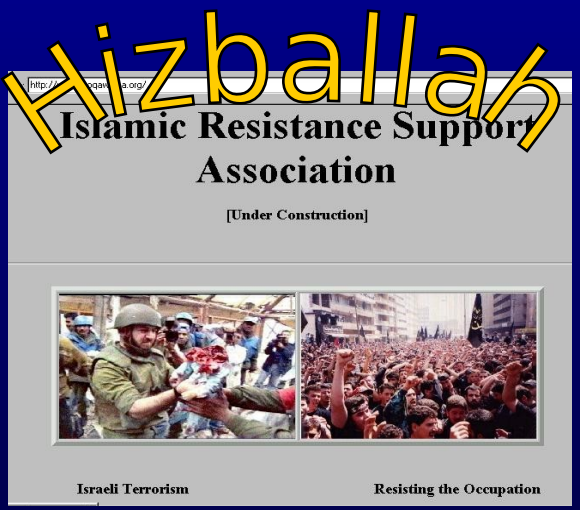
The Threats

EXTERNAL

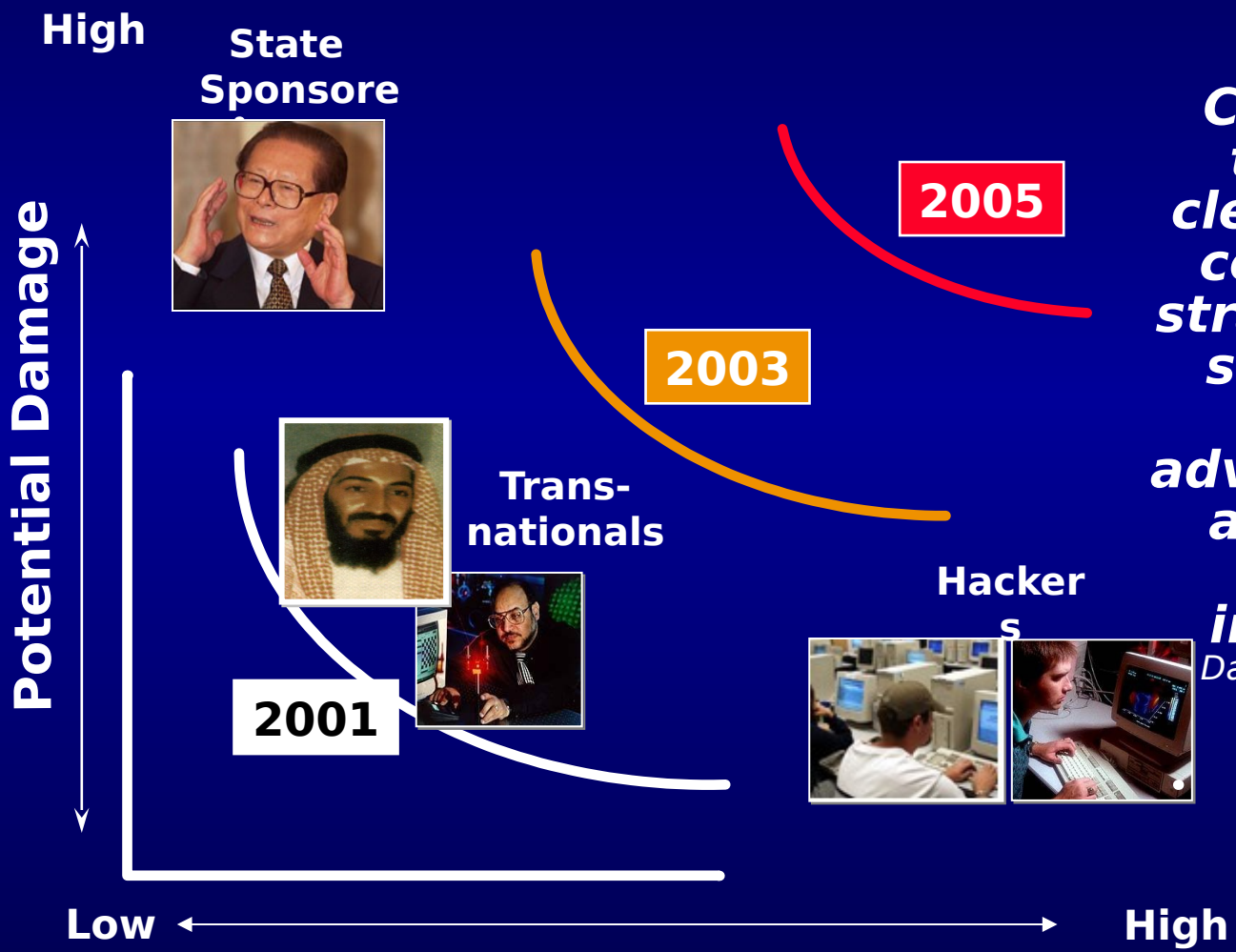
- Terrorists
- Drug-traffickers
- Organized crime
- Transnational
- Nation-State actors
- Hackers / Crackers / Crooks

INTERNAL

- Disgruntled employees
- Agents
- Unintentional errors



The Threat
The Spectrum

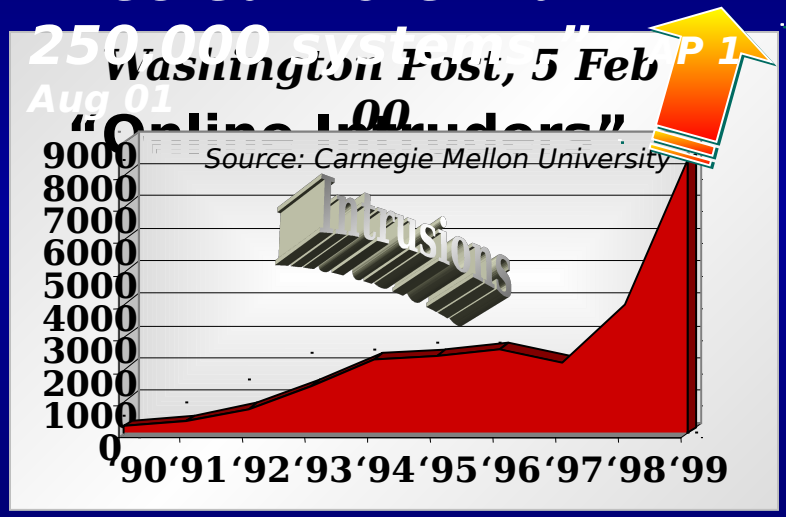


"Russian and Chinese military theorists have clearly enunciated computer attack strategies aimed at sowing fear and crippling an adversary's military and commercial information infrastructure."

Dan Kuehl, National Defense University

The Threat
The Fight is On

*"In just the first nine hours of its July 19 outbreak, **Code Red** infected more than 250,000 systems."* CP 1 Aug 01



*"Love Bug (caused) an estimated **$8 billion** in damage."*

WP, 11 May 00

CNN, 8,9,10 Feb 00

"Cyber-attacks batter Web heavyweights"

CNN.com
YAHOO!
amazon.com
ebay
buy.com

5 May 00

"FBI investigates 'ILOVEYOU' us; millions of computers affected"

"War in Kosovo and peacekeeping functions will cost the United States $6.7 billion through 2001" UPI, 2 Feb 00

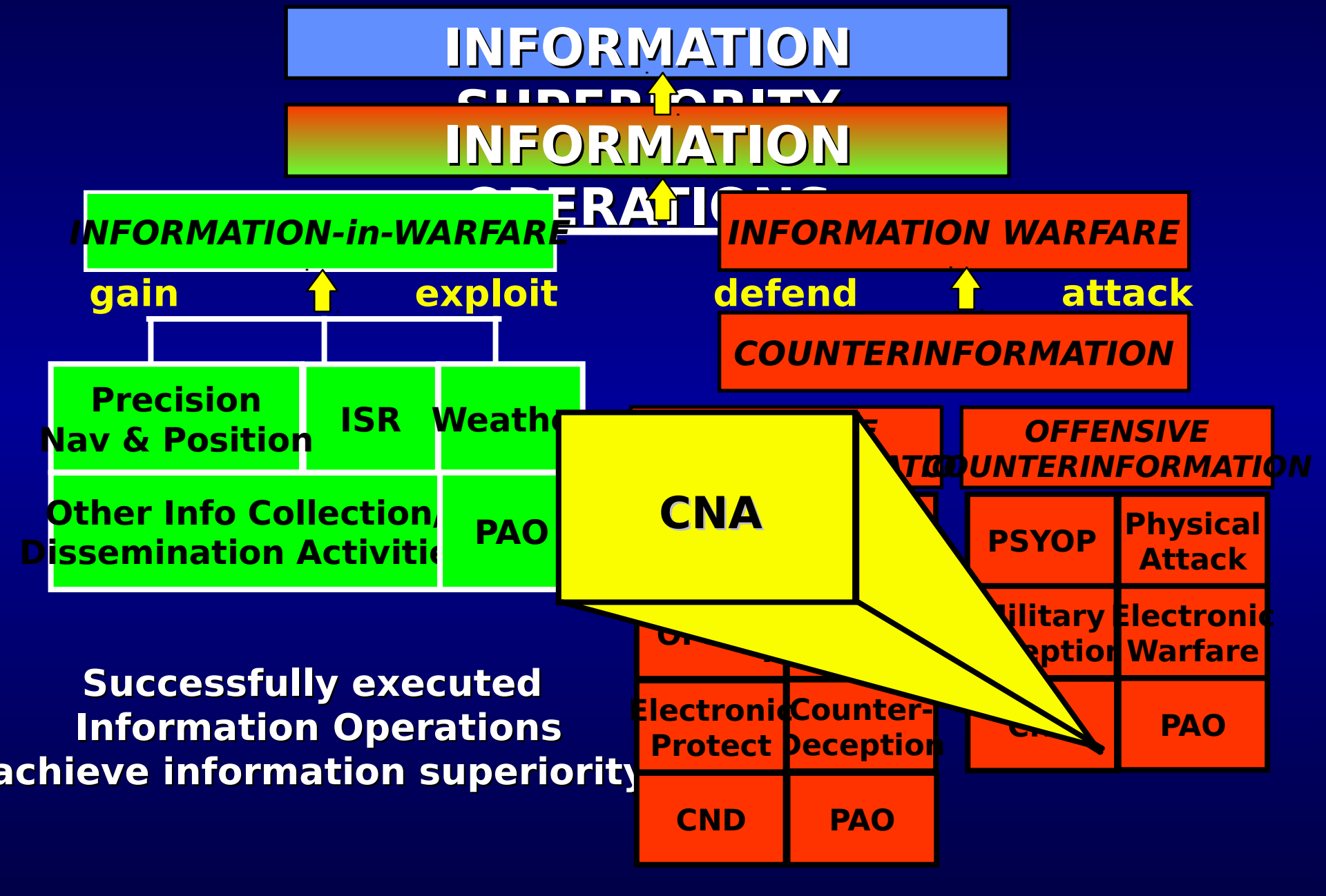
The Threat
"Chinese IW Doctrine"

"Strong countries make the rules while rising ones break them and exploit the loopholes…..War in the age of technological integration and globalization has eliminated the right of weapons to label war and, with regard to the new starting point, has realigned the relationship of weapons to war…..Does a single "hacker" attack count as a hostile act or not?…..Did CNN's broadcast of an exposed corpse of a U.S. soldier in the streets of Mogadishu shake the determination of the Americans to act as the world's policeman, thereby altering the world's situation? …..When we suddenly realize that all these non-war actions may be the new factors constituting future warfare, we have to come up with a new name for this new form of war: [illegible]scends all boundaries and limits, in [illegible] warfare."

Colonels Qiao Liang and

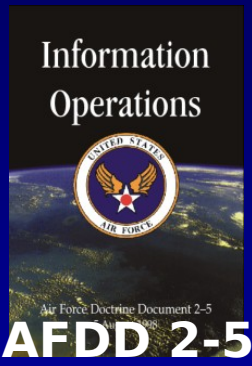
The Threat is Real

AFDD 2-5



Successfully executed Information Operations achieve information superiority

Computer Network Attack



AFDD 2-5

...operations conducted using information systems to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computers and telecommunication system are the principle means to employ CNA an are primary targets of CNA operations.

CNA Goals

- Alter information to affect decision making
- Destroy the enemy's confidence in the system
- Force an adversary to use less technical, and in most cases, less secure means to disseminate critical information
- Allow information to be exploited by friendly forces

CNA Benefits

Used not only in combat, but also before.

It offers …

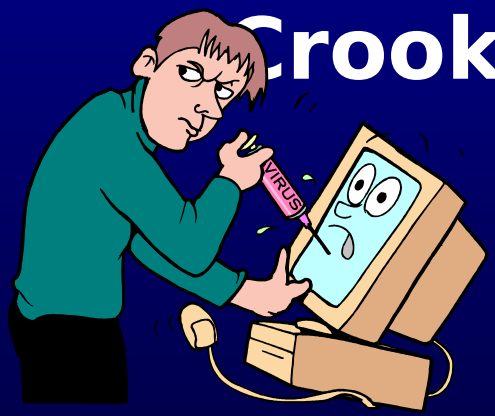
- **Ability to incapacitate an adversary early**
- **Reduce collateral damage**
- **Prevent adversary and friendly losses**

CNA capabilities and tools can save conventional sorties for other targets

The Adversary

All sorts of people want your info

- Curious
- Hackers / Crackers
- Telephone phreaks
- Crooks



WHY?

The Arsenal

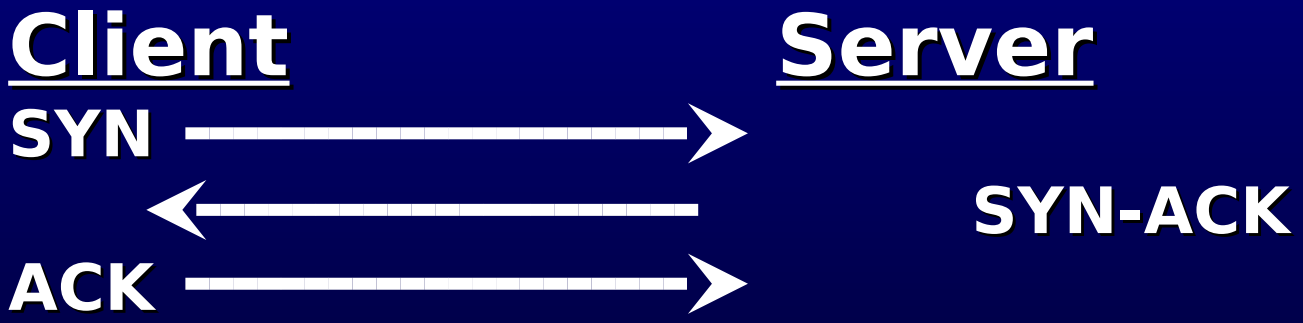
- Clandestine Code
- Denial of Service
- Backdoors
- Sniffers
- Chipping
- Malicious Software

Clandestine Code

- Allows programmers to insert code into the system that creates trapdoors; usually harmless
  - Word
  - Excel
  - what else….?

Denial of Service (DOS)

- Explicit attempt by attackers to prevent legitimate users of a service from using that service
  - attempts to flood a network, preventing legitimate network traffic
  - attempts to disrupt connections between two machines, preventing access to a service
  - attempts to disrupt service to a specific system or person



Backdoors
(aka Trapdoors)

- Mechanism that's built into a system by its designer
  - provides a way to sneak back into the system, circumventing normal system protection
  - what if …all US software could be equipped with a trapdoor that would allow IW agencies to explore systems and the stored data on foreign countries?

Sniffers

- Essentially a program that eavesdrops on network traffic.
- A sniffer looks for packets carrying login information.
  - they run “silently”; the software is simply watching packets go by without sending anything itself
  - they are essentially packet analyzers; common tools that have been in world-wide use for years

Chipping

- Making electronic chips vulnerable to destruction by designing in weaknesses
  - the chips could be built to so they fail after a certain time
  - blow up after they receive a signal on a specific frequency
  - send radio signals that allow identification of their exact location

How do we get the “right” people to use the affecte

Malicious Software

- **Virus/Worm: code fragment that copies itself into a larger program, modifying that program**
  - **‘86 = less than 10 known**
  - **‘90 = new one every 2 days**
  - **‘95 = 6,800+**
  - **‘01 = 57,000+**
  - **‘97 = 14,137+**
  - **‘98 = 21,000+**

Malicious Software

- **Virus/Worm**: code fragment that copies itself into a larger program, modifying that program
  - ‘86 = less than 10 known
  - ‘90 = new one every 2 days
  - ‘95 = 6,800+
  - ‘01 = 57,000+
  - ‘97 = 14,137+
  - ‘98 = 21,000+
- **Trojan Horse**: code fragment that hides inside a program and performs a disguised function
- **Logic Bomb**: a type of Trojan Horse, used to release a virus, a worm or some other system attack

Scanner Shortfalls

- **No scanner is 100% accurate or effective**
  - **They can only detect known viruses**
- **New viruses appear daily and may be undetectable**
  - **Updates to software are usually every month to month-and-a-half**

Attack Example...

Step 1.

A port scan finds active services on various systems

Step 2.

Attacker exploits weakness in a service to get root access on system outside the firewall. Covers tracks by deleting audit logs

Step 3.

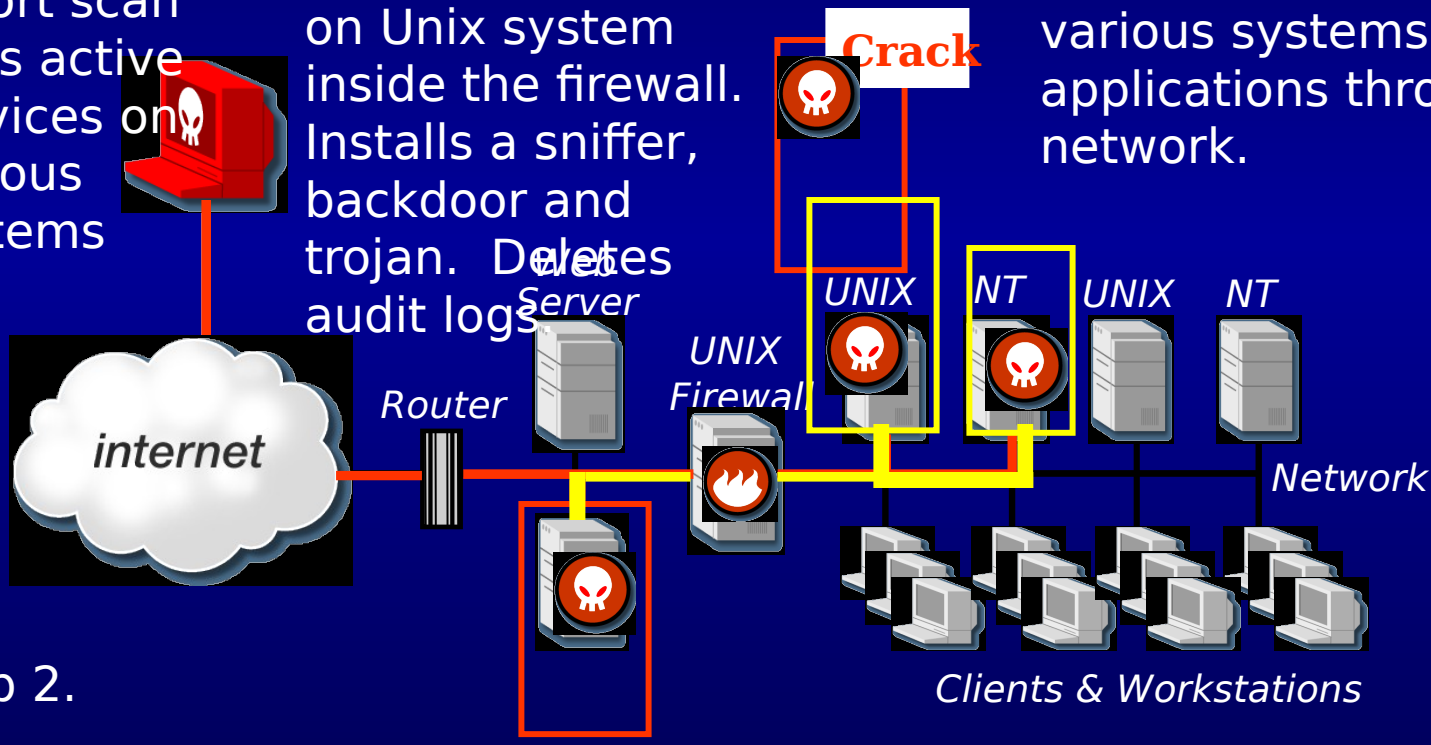
Attacker exploits trust relationships to gain root access on Unix system inside the firewall. Installs a sniffer, backdoor and trojan. Deletes audit logs

Step 4.

Attacker cracks password files and now has root/administrator access to various systems and applications throughout the network.

Step 5.

Attacker uses NT Admin password to access other systems

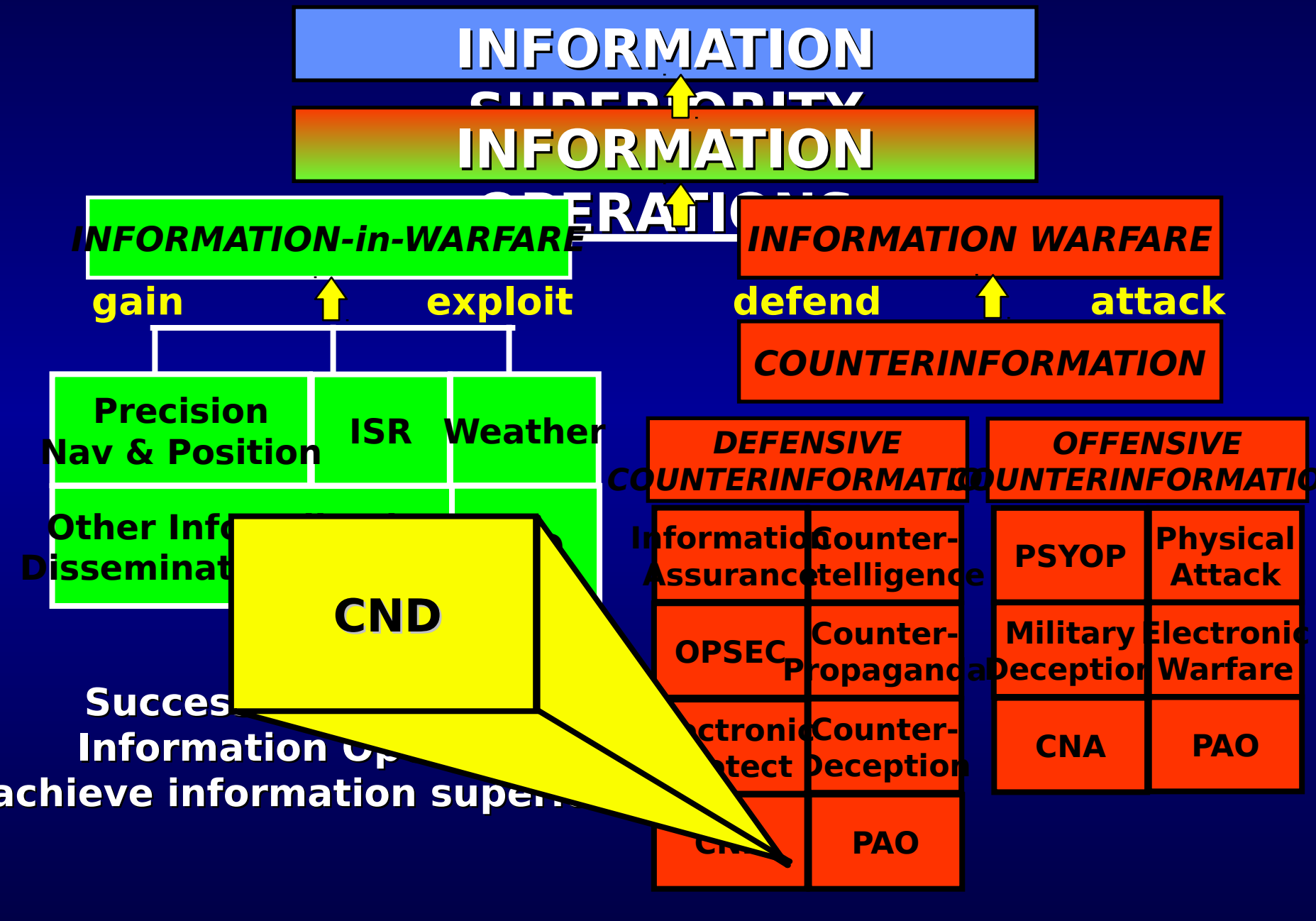


Disguised Attacks

“ Hackers are scapegoats…… Hackers are also far too loud and attention-seeking to be anything more than an annoyance, because they always end up talking or drawing attention to themselves somehow. Industrial spies and saboteurs do not. You will never see them, you will never know they were there.”

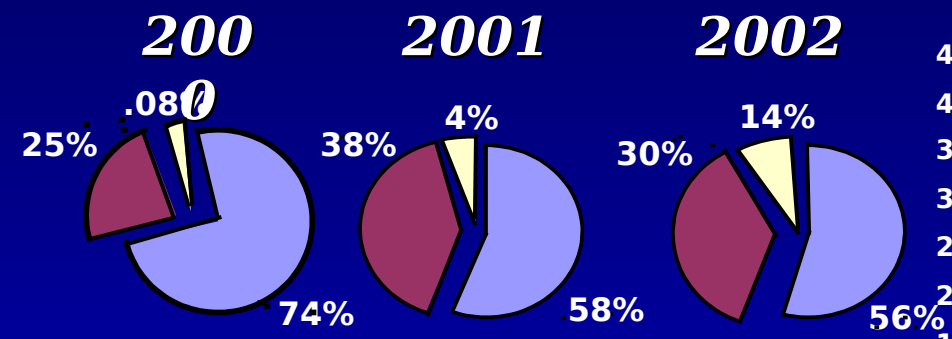
Chris Goggans (aka Bloodaxe)

AFDD 2-5


INFORMATION
INFORMATION
INFORMATION-in-WARFARE
gain
exploit
Precision Nav & Position
ISR
Weather
Other Info
Disseminat
INFORMATION WARFARE
defend
attack
COUNTERINFORMATION
DEFENSIVE COUNTERINFORMATION
OFFENSIVE COUNTERINFORMATION
Information Assurance
Counter-intelligence
OPSEC
Counter-Propaganda
Counter-Deception
PAO
PSYOP
Physical Attack
Military Deception
Electronic Warfare
CNA
PAO
CND
Succes
Information Op
achieve information super

Increasing Level of Detected Activity

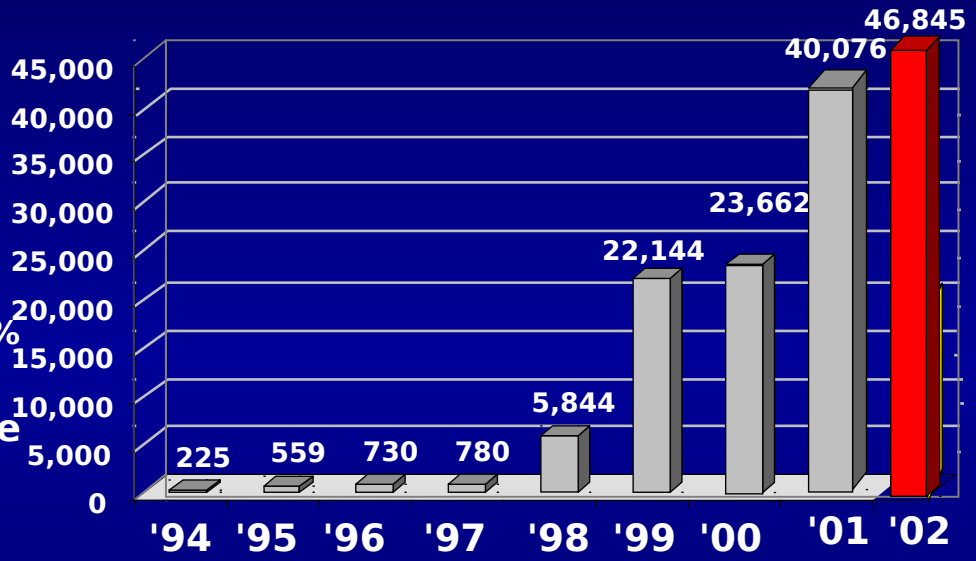
Root & User Level Access 2.5 Million Computers DoD Wide



- IAVA/Technical Bulletins Published (56%)
- "Poor Security Practices" (30%)
- "New" Intrusion Method (14%)

Level of Detected Activity

(DOD Unclassified Network "NIPRNET")



More Detection

- Intrusion Detection
- Organization/Reporting
- Awareness/Training
- Network Hardening

+

More Intrusions

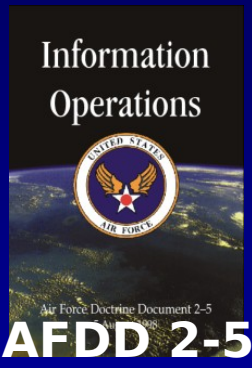
- More Tools
- Better Organization
- Publicity
- Politics/Protest

Sound easy to FIX?

What does it mean to have 5500 vulnerabilities reported in 2002?

- **somebody has to read the descriptions of the vulnerabilities**
  - ***5500 * 20 minutes* to read = *229 days* just to read the descriptions.**
- **suppose you're affected by *10%***
  - ***550 vuls * 1 hour* to install the patch = *69 days* just to install patches on one machine**
- **just to read security news and patch a single system *229 + 69 = 298 days***

Computer Network Defense



AFDD 2-5

… actions taken to plan and direct responses to unauthorized activity in defense of Air Force information systems and computer networks.

Actions include analyzing network activity to deter the appropriate course of action to defend Air Force networks. Often this task will require fusion with information assurance activities, intelligence info, counterintelligence info, and operational considera to determine the nature of the threat to friendly sy

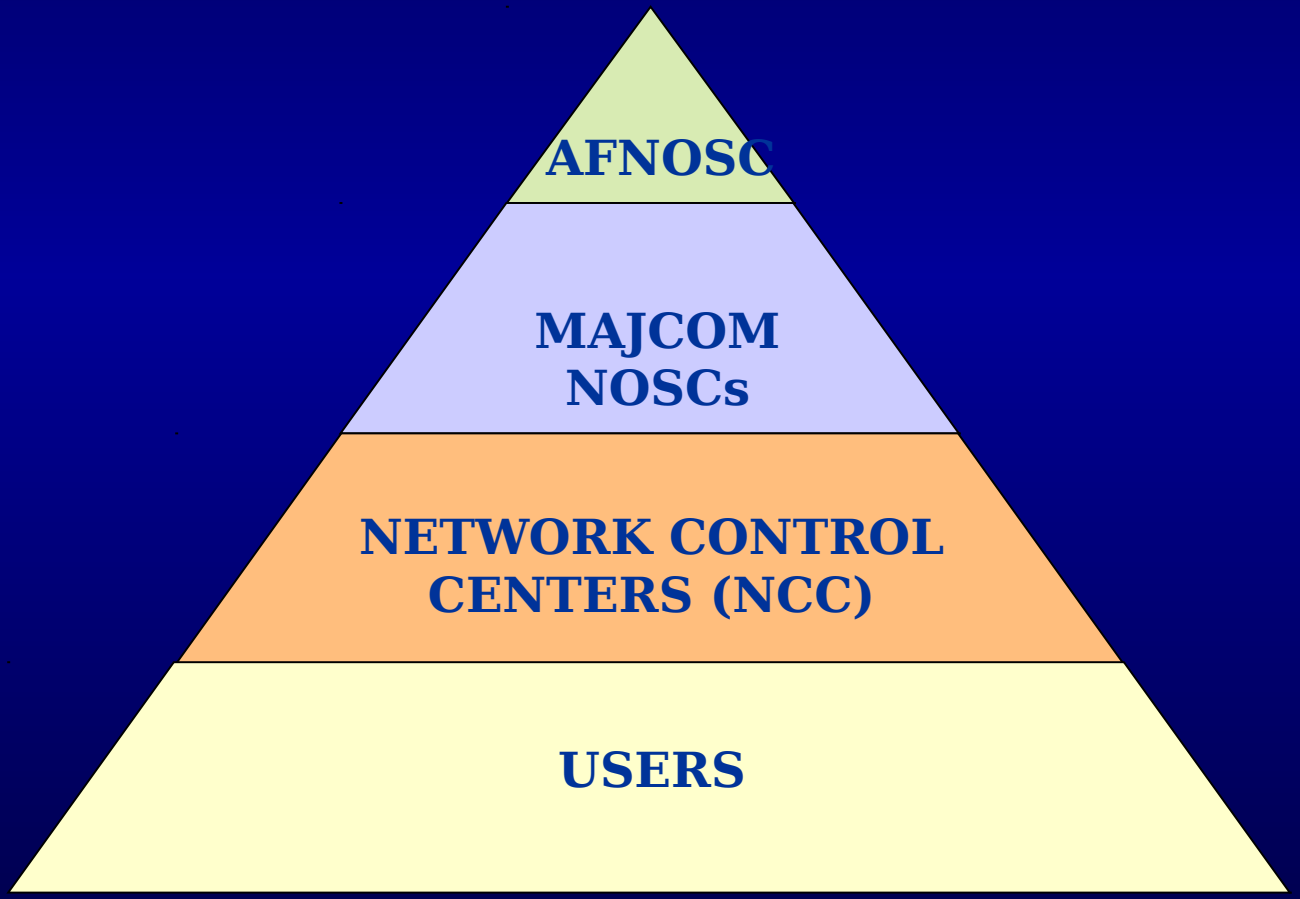
NCC / NOSC / AFNOC

- **NCC:** Network Control Center - base level
  - Performs fault, performance, configuration, accounting, network and security management
- **MAJCOM NOSC:** Network Operations and Security Center - MAJCOM level
  - Provides perimeter defense capabilities, intrusion detection, internal controls, recovery from damages, and protection from denial of service attacks
- **AFNOSC:**
  - Air Force Network Operations Center - AF level
    - Manage base-level service delivery point routers to provide enterprise view across AF networks
  - AFCERT - AF level
    - Monitor AF network traffic and coordinate computer network defense actions

Formation of the AFNOSC

"26 Feb 03, CSAF approved the AFNOSC"

(8th AF COMAFFOR-CNO + AFNOC + AFCERT)



AFNOSC Computer Network Defense

AFNOSC Event Correlation

AFNOC
AF Network Operations Center

- Systems Management & Configuration
- Intrusion/Malicious Logic Detection
- Firewall Management
- Network Health
- Base Assistance

SUPPORTING the JTF-CNO

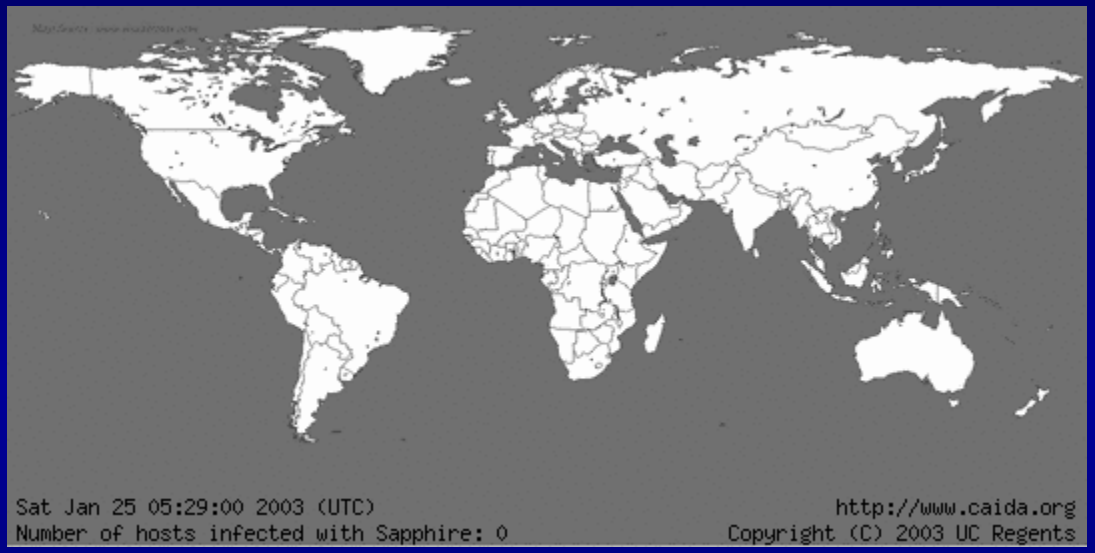
AFCERT
AF Computer Emergency Response Team

- Intrusion/Malicious Logic Detection
- Incident Response
- Computer Security Information Assurance
- Vulnerability Assessment of AF AISs

Sensors	Reporting	Analysis

Defense and Protection of the AF Enterprise Netw

CND: AF Reaction to Slammer Worm



- Globally blocked network addresses
  - Stopped attacks at AF gateways—prevented cross contamination
  - Reduced workload on AFCERT sensors
- AFCERT & AFNOC isolated infections and control fix actions

Stay Current

How / Who do you report problems / issues?

- **Workgroup Manager / ISSO**
- **Unit COMPUSEC Manager (UCM)**
- **Base COMPUSEC Manager @ WIPO**

AF Publications on Communication & Information (33 Series):
http://afpubs.hq.af.mil

Organizations

USSTRATCOM JTF-CNO

- Assigned CND mission - Oct 99
  - Coordinate joint, combined, civil, and commercial efforts to protect/defend computer networks vital to national security

- Assumed CNA mission - Oct
  - Synchronized joint operations to gain and exploit information superiority and denial of adversary ability to do the same

JTF-CNO CONOPS being developed

92 IW Aggressor Squadron (318IOG, AFIWC)

MISSION:
Conduct Opposing Force IW operations and IW vulnerability assessments by replicating threat capabilities and tactic

Squadron CONOPS

- Train warfighters to apply IW combat power
- Replicates realistic threat
- Supports real world operations and exercises

'99 - '00 Assessments

Site	Total Systems	Penetrated Systems	Pct %	Root Access	High Risk Vul	Low Risk Vul
A	10	10	100	8	15	8
B	33	33	100	17	26	12
C	210	190	90	183	19	12
D	26	25	96	6	14	7
E	102	94	92	94	18	2
F	7	7	100	7	11	8
G	9	9	100	3	10	6

Systems - network devices, i.e., workstations, servers, routers, printers

High Risk Vulnerabilities: potential for most privileged access

Low Risk Vulnerabilities: user/system info gathered, user level access

Air Force Computer Emergency Response Team

- Detect and prevent computer/network intrusions
- Rapid incident response
- AF-level anti-virus analysis and support
- Research computer vulnerabilities

AFCERT is the execution arm for the COMAFFOR JTF-CNO

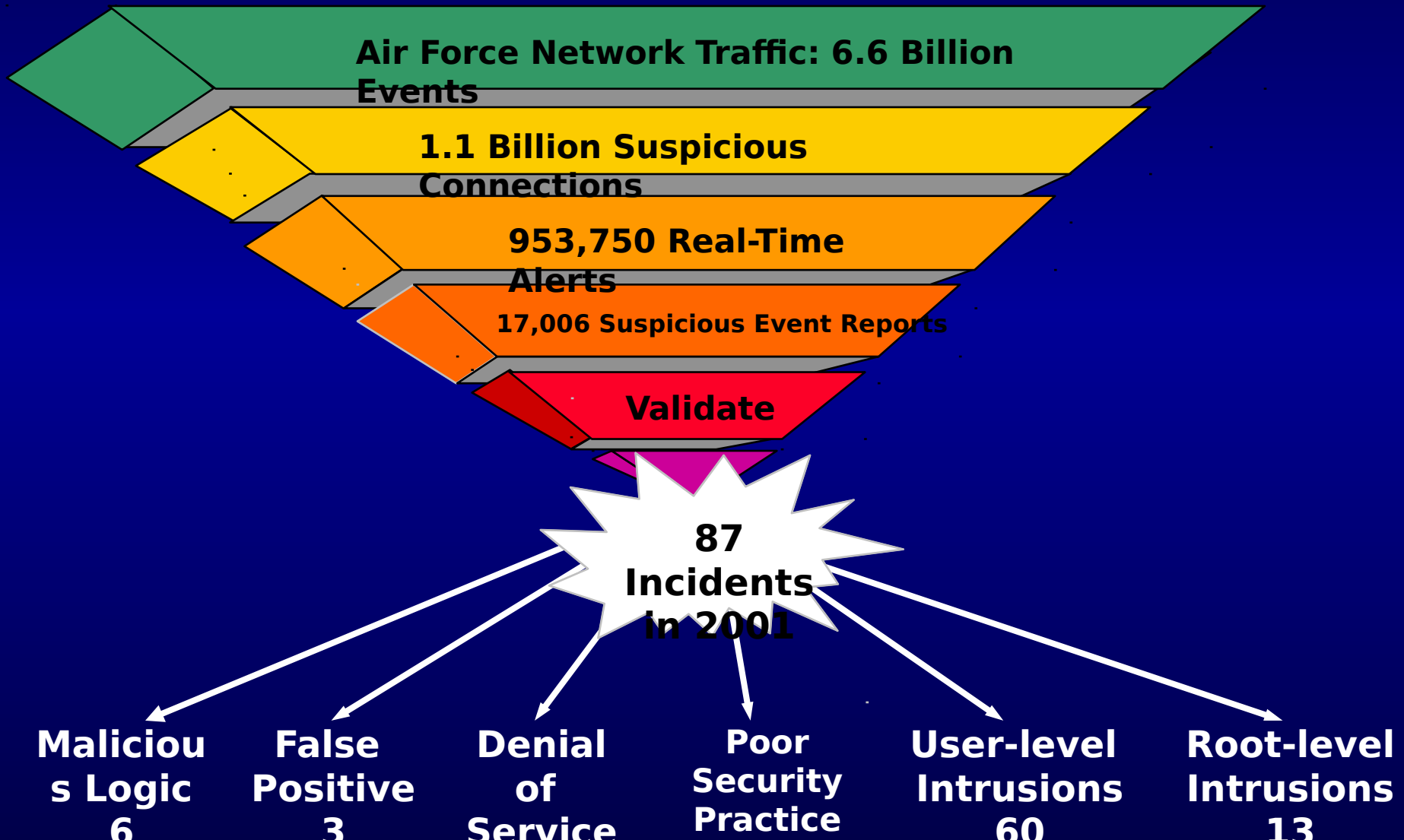
AFCERT

https://afcertmil.lackland.af.mil
DSN 969-3157
1-800-854-0187
(210) 977-3157

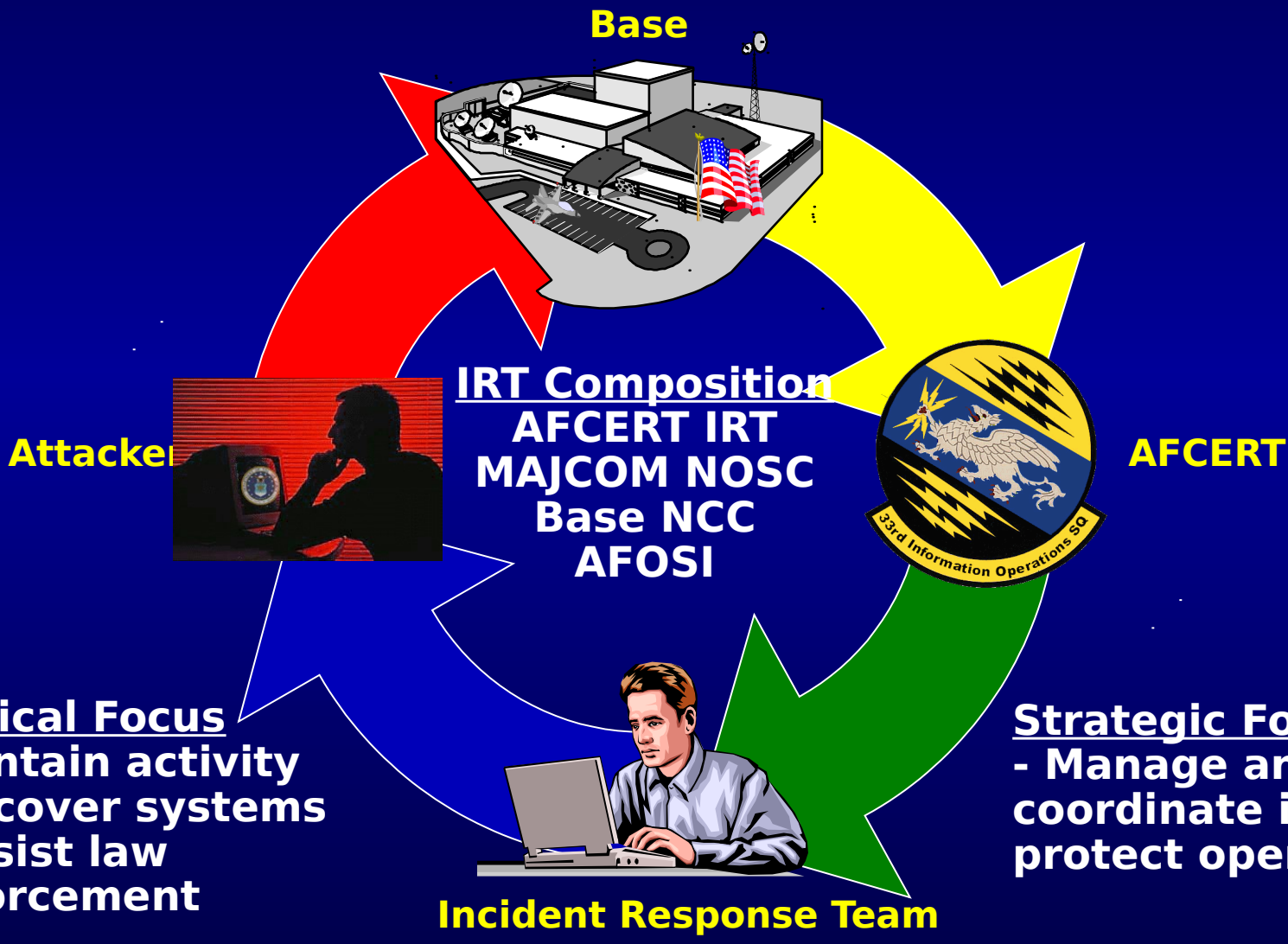
Intrusion Detection

- **Purpose**
  - **Monitor Air Force and other customer networks (USCENTCOM) for suspicious activity**
- **Operational Goal**
  - **Detect and prevent compromise of Air Force and other customer computers and networks**
- **Defensive Weapons Platforms**
  - **Automated Security Incident Measurement (ASIM) sensor (GOTS)**
  - **Cisco Secure Intrusion Detection System (COTS)**

Intrusion Detection: Traffic Load



Incident Response Team



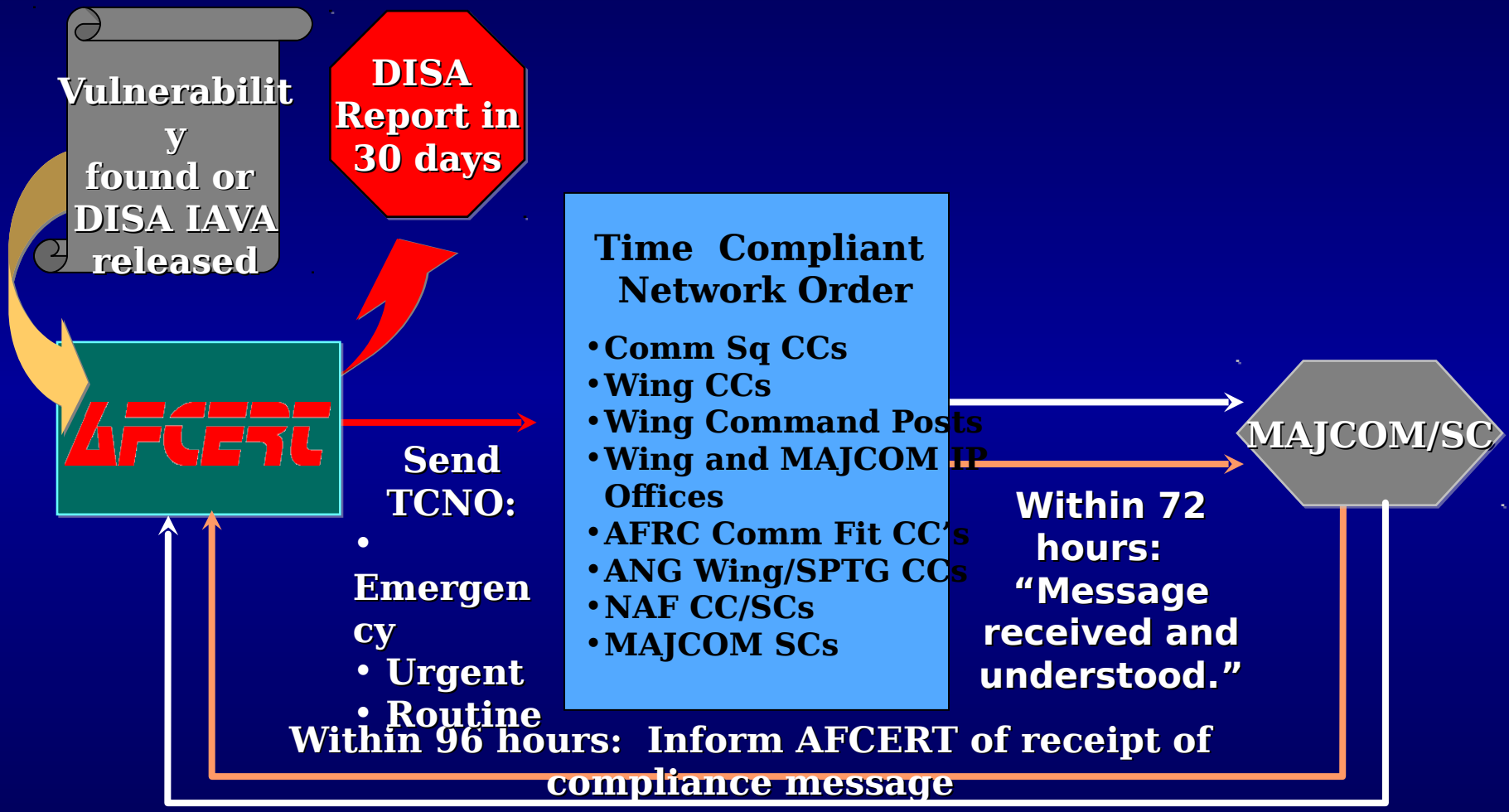
Virus Analysis

- **Identify, analyze, and respond to new virus threats**
  - **Anti virus Signature Files**
  - **Sensor Strings**
- **Verify and report virus activity on AF networks**

Vulnerability Analysis

- Identify and analyze vulnerabilities of AF networks
- Recommend / mandate proactive measures to AF units
- Notify AF on availability and location of software patches
- Publish and monitor Time Compliance Network Order (TCNO) process

Vulnerability Mitigation



Inform AFCERT of compliance with fix actions; exceptions are also outlined

Emergency: <= 27 days, Urgent: <= 57 days, Routine: <= 87

USAF Defensive Counterinformation (DCI) Fusion Center

Mission

The USAF Defensive Counterinformation (DCI) Fusion Center will provide full-spectrum fused DCI products and services to all USAF organizations' global operations.

DCI Fusion Center Mission

- **Gather** - DCI event reports from world-wide USAF operations and intelligence communities
- **Analyze** - Fuse DCI events to determine any linkages
- **Report** - Format analysis to provide situational awareness to support defensive courses of action and risk management options
- **Disseminate** - Provide reports to all AF commanders at all levels and applicable Joint/National Agencies via DCI NOTAMs

DCI disciplines

- Information Assurance
- Computer Network Defense
- OPSEC
- Counter-Propaganda
- Public Affairs
- Counter-Intelligence
- Counter-Deception
- Electronic Protection

Products & Services

- Weekly XOI DCI Report
- AOR DCI Full Spectrum Analysis
- AFCERT/AFNOSC Weekly Report
- Annual Reports
- Periodic Fused Analysis Reports
- Annual World-wide DCI Conference
- Event Reports
- DCI Reports
- DCI Assessments
- Risk Management Options
- Advisories
- Assist Metric Development & Yearly Evaluation
- DCI Doctrine Development

Summary

- CNA
  - Definition
  - The Threat
  - The Arsenal
- CND
  - Definition
  - Structure
- Organizations

Why do it?

**"I don't care how many millions of dol
you spend on hardware, if you don't h
people trained properly I'm going to g
if I want to get in."**

Hacker, Cyberpunk Magazine